VERMONT INTELLIGENCE CENTER
188 HARVEST LANE
WILLISTON, VT 05495
PHONE: 802-872-6126 FAX: 802-872-6125
EMAIL: DPS.VIC@state.vt.us

15-CIVIC-21 | **CYBER ADVISORY** | February 25, 2015

UNCLASSIFIED

Dissemination is restricted to those who have law enforcement or public safety responsibilities, or to individuals who have a need to know/right to know based on the execution of their official duties in order to protect the public. This includes critical infrastructure partners whose position or role gives them a need to know/right to know.

(U) "Anonymous" calls for targeting of FBI Call Centers and Child Protective Services – May Impact State/Local Law Enforcement Call Centers

(U) The hacktivist group "Anonymous" recently posted a message on Pastebin[dot]com calling for their supporters to disrupt law enforcement call centers on March 21st, 2015. Anonymous indicated they intend to bring awareness to alleged corruption within child protective service related agencies through their effort. The organization also calls upon hackers to exploit vulnerabilities found on child protective service related websites to bring visibility to their cause – the perceived exploitation and trafficking of children by Child Protective Services (CPS) for profit.

(U) The posts (#OpExposeCPS) outline plans to conduct Telephonic Denial of Service (TDoS) attacks on the FBI's public phone number and calls for additional attacks on state law enforcement agencies. The stated goal is to inundate the FBI's phone lines severely enough to bring media attention to their underlying cause.

(U) Once the TDoS against the FBI call center "succeeds", the group urges callers to target additional "state BI's" – which is believed to be an abbreviation for state Bureau of Investigations. The attackers may treat other law enforcement agencies as secondary targets.

(U) On February 10, 2015 the original Pastebin[dot]com post was amended to include the following:

We have added more phone numbers to the target list. The FBI released the corruption hot-line mid December, so since we are dealing with corruption of the most disgusting kind, what better place to start. We also have missing and exploited child numbers to take advantage of. And of course there is the main call center of the FBI. If you have never called this number before you will be directed through a series of questions to get to the best department to take your call. We intend to flood them all.

We are also asking for people to send in faxes to the fax tip line. There are many ways to do this from using a real fax machine to online services that will send faxes for you. In the coming weeks we will put together a bunch of faxes that can be used, these can also be used for emails as well. Most will be a 2 page document containing a picture and information about the victim or case relevant to the picture. Make sure you fax them in black and white. ;)

[*]A few links to help you with talking points for the call[*]

https://www.youtube.com/watch?v=1zKKkVrLpzc

https://www.youtube.com/watch?v=I0OiNdj2aP4

https://www.youtube.com/watch?v=HVaOzM6tVNc

(U) The event page can be found at the following: https://www.facebook.com/events/640635849381607

VIC NOTE: This information is being provided for situational awareness purposes only. Distributed Denial of Service (DDoS) attacks against major websites is not endorsed or recommended by organizers. However, direct intrusions against CPS systems are encouraged as a method for obtaining or leaking sensitive information. IT security personnel managing law enforcement or CPS networks/systems should anticipate an increase in activity leading up to March 21st.

VIC NOTE: It is likely that supporters will begin conducting penetration testing or web defacements prior to March 21st. At this time the Vermont Intelligence Center has no credible information to indicate Vermont law enforcement and/or the Vermont Department of Children and Families (DCF) has or will be targeted. Targets specifically identified to-date include the FBI's National Call Center, the National Center for Missing and Exploited Children's (NCMEC) 24-hour Tip Line and the FBI's national public corruption tip-line.

(U//FOUO) HACKTIVISTS THREATEN LAW ENFORCEMENT OFFICIALS

For comments or questions, contact the Center by phone at (802) 872-6126 or e-mail at DPS.VIC@state.vt.us

14-CIVIC-9

(U//FOUO) With the on-going events occurring in Ferguson, MO, police agencies should be aware of the increased risk of cyber-based attacks when there is a perceived injustice. Attacks can be precipitated by someone scanning networks or opening infected emails containing malicious attachments or links.

(U//FOUO) Officers should be aware of their online presence and exposure. Officers have posted images wearing uniforms that show name tags or list their police department on social media sites. This information can increase an officer's risk of being targeted or attacked. Many legitimate online posts are now linked directly to personal social media accounts. Everyone needs to maintain an enhanced awareness of the content they post and how it may reflect on themselves, their family, and their employer or how it could be used against them in court or during online attacks.

(U) DOXING

(U) The act of someone posting an individual's personal information without permission is known as "doxing".

(U) The personal information gathered from social media and other websites could include the individual's home address, phone numbers, email addresses, passwords and any other information used to target them. The information is then posted on sites such as "Twitter" and "Pastebin.com" with details as to why the individual should be targeted.

(U) On-going trends suggest that law enforcement officers' families are also very open to attacks and doxing activity. This includes the posting of pictures and personal information on these same social media websites.

(U) DEFENDING AGAINST HACKTIVISM

(U) While eliminating your exposure in the current digital age is nearly impossible, everyone can take steps to minimize their risk in the event they are targeted.

(U) Turn on all privacy/security settings on social media sites, home computers & wireless networks and refrain from posting pictures showing your affiliation to law enforcement Advise family members to do the same.

(U) Pay close attention to all work and personal emails, especially those containing attachments or links to other websites. These suspicious or phishing emails may contain infected attachments or links.

(U) Enable additional email security measures to include two factor authentication on your personal email accounts. This is a security feature offered by email providers including Gmail, MSN and Yahoo mail. The feature will cause a text message to be sent to your mobile device prior to accessing your email account.

(U) Limit your personal postings on media sites and carefully consider comments.

(U) Routinely update hardware and software applications, including antivirus.

(U) Closely monitor your credit and banking activity.

(U) Restrict your driver license and vehicle registration information with the Department of Motor Vehicles.

(U) Request real estate and personal property records be restricted from online searches with your specific county – Department of Revenue.

If you've fallen victim to a scam, immediately notify the FBI's Internet Crime Complaint Center (IC3) - www.IC3.gov

Published August 18, 2014

VERMONT INFORMATION & ANALYSIS CENTER
188 HARVEST LANE
WILLISTON, VT 05495
PHONE: 802-872-6110 FAX: 802-872-6125
EMAIL: VTFUSION@DPS.STATE.VT.US

13-VTIAC-0184 | INTELLIGENCE BULLETIN | March 18, 2013

Anonymous Threatens to Dump Credit Card Details of Many from Law Enforcement

The hacktivist group Anonymous posted a Twitter announcement on March 15, 2013 expressing a plan to publicize personal and financial information obtained on law enforcement officers, including railroad police.
Anonymous claims the data includes the credit card account numbers and social security numbers of individuals identified in various databases the group has compromised. The organizations from which this information has been stolen have not, as yet, been identified. As a result, it remains uncertain which, or how many, individual law enforcement officers may be affected by this security breach - and thereby potentially exposed to fraudulent misuse of personal and financial information.

As a precaution, railroad and transit police officers should be encouraged to closely monitor their bank and credit card accounts for any unusual activity, including indications of purchases they have not made. In so doing, one option is to contact the financial institutions that maintain their credit card, checking, and saving accounts to arrange for an alert to any activity that seems suspect because it departs from normal usage.

The following references provide details on the information posted by Anonymous that prompts this advisory:

1) From the Pastebin post: *"We have access to a number of law enforcement databases and systems of companies that earn their money from law enforcement funds.*
We are sitting on a lot of data, with complete credit card details and in some cases social security numbers as well.
<Note: emails and other personal identifying information posted on the site have been redacted. >
These databases have enabled us to put together a lot of cop dox, couple examples below for our porcine friends.
This data will be released, there are no ultimatums here."

2) The Hacker News reported: Anonymous threatens to dump credit card details of many from law enforcement. According to a post published online via Anonymous hackers, they are claiming to have credit card details and Social security numbers of many people from various law enforcement agencies. Hacktivist demanding the release of all anonymous members, arrested last year. "Jeremy Hammond has already served over a year behind bars, held without bail at MCC New York.", "Barrett Brown is facing 3 separate rounds of charges relating to a crazy you tube video, a poorly hidden laptop and linking to a database dump in an IRC channel." , "Matthew Keys has just been indicted for supposedly sharing admin login details of the Tribune Company with SABU over two years ago. The law will target those around and within Anonymous in any way that they can, and bottom feeders like sabu will help prop up any flimsy case they happen to want to bring." At last, hackers threaten to dump whole data online.

(http://news.thehackernews.com/anonymous-threatens-to-dump-credit-card-details-of-many-from-law-enforcement)

3) Twitter announcement:
Anonymous@YourAnonNews
#Anonymous threatens to dump credit card details of many from law enforcement
http://bit.ly/YgqwBG #FTP #FreeAnons #FreeMattKeys #FreeBB